Preface

The International Electrotechnical Commission Advisory Committee on Safety puts out a Guide, ISO/IEC Guide 51, for the inclusion of processes concerned with safety in any electrotechnical standards which have safety aspects. Guide 51 says to require the performance of

- hazard identification (find the hazards),
- hazard analysis (examine their possible consequences),
- risk analysis (put those consequences together with the likelihood they will be realised in operation).

There is also a general requirement that

- incidents and accidents in operation of a system be causally analysed

which comes from due-diligence requirements, often incorporated specifically into national and sometimes international law.

This textbook presents these four techniques, using methods which have been developed by myself and my group at Bielefeld University since 1995, as well as at the tech-transfer companies Causalis Limited and Causalis Ingenieurgesellschaft mbH. Those methods are Why-Because Analysis (WBA); Objects, Properties, Relations and Assertions Analysis (OPRA), Ontological Hazard Analysis (OHA) and Causal Fault Analysis (CFA). We have no unique methods for risk analysis per se, but the two chapters on risk analysis incorporate some novel approaches.

The book is intended for use primarily in university courses or industrial short courses, but I would like to encourage the enterprising engineer to study it and try the exercises on her own when such courses are not locally available. There are a lot of tables and lists involved, and relatively few pictures (as in graphs). This just seems to be so in hazard and failure analysis. There might be a temptation to consider system safety as just a matter of filling out such tables carefully, but I hope to have shown here by example that it is much more than that.

Many people have contributed to this work over the years, and I thank them all. The first example of WBA used as a rigorous formal method was in the Diplom thesis of Karsten Loer. Bernd Sieker and Jan Paller put together the first SW support toolkit for WBA, YBT, which Causalis used in industrial tutorials in Europe and Australia. Jan Sanders put together the second toolkit, YBT2, and Hauke Kaufhold has recently modified this to YBT3, part of the SERAS toolkit. The SERAS Reporter, which generates factors for input to YBT2 and YBT3 from a running-text prose description of a situation, was originated by Jan Sanders on the basis of a parser by Dafydd Gibbon, and further developed by Sören Bollmann. Jörn Stuphorn put together the first version of a SERAS report generator for presenting a completed WBA in a document. Lars Molske developed a WBA tool based on a sophisticated parser for a Controlled English dialect, and Damian Nowak wrote a tool for comparing two Why-Because Graphs, in particular of the same incident put together by different teams, and harmonising them. Bernd Sieker produced a model example of OHA for his PhD thesis – would that all applications could proceed as straightforwardly as this! Hauke Kaufhold and Tim Schürmann developed the communications-bus OHA a number of levels further on. The risk analysis example of charging systems for electric road vehicles owes a great deal to discussions over the course of a couple of years with participants in DKE Working Group AK 353.0.5. I owe particular thanks to Bernd Sieker for the many industrial projects we worked on together at Causalis, during which the techniques presented here matured. Bernd was also a member of DKE AK 353.0.5 and authored a discussion document in German.

Peter Bernard Ladkin
Bielefeld, December 2017